(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7489069号
(P7489069)

(45)発行日　令和6年5月23日(2024.5.23)

(24)登録日　令和6年5月15日(2024.5.15)

(51)国際特許分類		FI		
H04L	*9/36 (2006.01)*	H04L	9/36	
H04L	*9/32 (2006.01)*	H04L	9/32	200B
H04L	*9/08 (2006.01)*	H04L	9/08	C

請求項の数　11　（全14頁）

(21)出願番号　特願2021-562983(P2021-562983)
(86)(22)出願日　令和2年4月23日(2020.4.23)
(65)公表番号　特表2022-530406(P2022-530406A)
(43)公表日　令和4年6月29日(2022.6.29)
(86)国際出願番号　PCT/IB2020/053851
(87)国際公開番号　WO2020/217202
(87)国際公開日　令和2年10月29日(2020.10.29)
審査請求日　令和5年2月8日(2023.2.8)
(31)優先権主張番号　102019000006242
(32)優先日　平成31年4月23日(2019.4.23)
(33)優先権主張国・地域又は機関
イタリア(IT)

(73)特許権者　505252296
イタルデザイン－ジュジアーロ・ソシエタ・ペル・アチオニ
ＩＴＡＬＤＥＳＩＧＮ－ＧＩＵＧＩＡＲＯ Ｓ．ｐ．Ａ．
イタリア、イ－１０１２１トリノ、ヴィア・エッセ・クインティーノ２８番
(73)特許権者　506075182
ポリテクニコ ディ トリノ
イタリア国、１０１２９ トリノ、コルソ デュカ デグリ アブルッヅィ、２４
(74)代理人　100145403
弁理士　山尾 憲人
(74)代理人　100135703
弁理士　岡部 英隆

最終頁に続く

(54)【発明の名称】　ＳＯＭＥ／ＩＰ通信プロトコルを用いる乗物上におけるデータ又はメッセージの伝送の改良

(57)【特許請求の範囲】

【請求項１】

乗物のオンボードの通信ネットワークにおいて、ＳＯＭＥ／ＩＰ通信プロトコルを用いて、サービスインスタンスを要求する少なくとも１つの要求側エンティティと、サービスインスタンスを提供する提供側エンティティとの間でデータ又はメッセージを伝送するための方法であって、

上記提供側エンティティは、上記要求側エンティティによる要求の結果として応答を提供するか、又は、上記提供側エンティティは、周期的な通知、もしくは、上記要求側エンティティによるサービスへの加入の結果としてイベントによりトリガされた通知を提供し、

上記乗物の外部の証明手段によって、上記要求側エンティティ及び上記提供側エンティティの予め割り当てられた証明書の発行を通じて、上記少なくとも１つの要求側エンティティ及び少なくとも１つの提供側エンティティがサービスインスタンスにアクセスすることの認可が予め定義され、上記提供側エンティティの証明書は、複数の予め決められたセキュリティレベルのうち最低のセキュリティレベルを、上記提供側エンティティのためのサービスにさらに割り当て、上記要求側エンティティの証明書は、上記複数の予め決められたセキュリティレベルのうち最低のセキュリティレベルを、上記要求側エンティティのためのサービスに割り当て、

上記方法は、サービスインスタンスに関連付けられた後続の通信の開始部分を考慮した、上記要求側エンティティ及び上記提供側エンティティの間における準備的相互認証ステップを含み、上記準備的相互認証ステップは、

－　上記要求側エンティティ及び上記提供側エンティティの上記予め割り当てられた証明書の存在及び相互の有効性を検証することと、
－　上記提供側エンティティによってサービスが提供されるセキュリティのレベルが、上記要求側エンティティ及び上記提供側エンティティにおいて上記サービスに予め割り当てられた上記最低のセキュリティレベル未満ではないことを検証することと、
－　上記セキュリティレベルの検証及び上記証明書の検証に成功した場合、サービスインスタンスに関連付けられた少なくとも１つの通信メッセージを、上記提供側エンティティから上記要求側エンティティに、及びその逆に伝送することとを含む、
方法。
【請求項２】
　上記複数の予め決められたセキュリティレベルは、
　予め決められた暗号化関数で暗号化されたメッセージ認証コードがサービスインスタンスの通信の各メッセージに関連付けられる認証セキュリティレベルと、
　各通信メッセージが、予め決められた暗号化関数で暗号化されたメッセージ認証コードと、上記予め決められた暗号化関数で暗号化されたペイロードとを含む機密性キュリティレベルとを含む、
請求項１記載の方法。
【請求項３】
　上記予め決められた暗号化関数は、上記準備的相互認証ステップにおいて上記提供側エンティティによって上記要求側エンティティに伝送された各サービスインスタンスに関連付けられた対称暗号鍵を含む、
請求項２記載の方法。
【請求項４】
　上記メッセージ認証コードは、上記通信メッセージと上記サービスインスタンスに関連付けられた上記対称暗号鍵とを入力として受けて固定サイズのバイト列を返す上記予め決められた暗号化関数を用いて、送信側エンティティによって生成される、
請求項３記載の方法。
【請求項５】
　上記対称暗号鍵は、上記要求側エンティティの公開暗号鍵を用いて暗号化され、上記提供側エンティティによって上記要求側エンティティに伝送される、
請求項３又は４記載の方法。
【請求項６】
　上記提供側エンティティによってサービスが提供されるセキュリティのレベルが、上記提供側エンティティ及び上記要求側エンティティにおいて上記サービスに予め割り当てられた上記最低のセキュリティレベル未満ではないことを検証することは、上記提供側エンティティ及び上記要求側エンティティにおいて実行される、
請求項１～５のうちの１つに記載の方法。
【請求項７】
　上記準備的相互認証ステップは、
　上記予め割り当てられた証明書を含むか又は上記要求側エンティティの上記予め割り当てられた証明書の識別子を含む認証要求のためのメッセージを、上記要求側エンティティから上記提供側エンティティに送信することと、
　上記予め割り当てられた証明書を含むか又は上記提供側エンティティの上記予め割り当てられた証明書の識別子を含む認証応答メッセージを、上記提供側エンティティから上記要求側エンティティに送信することとを含む、
請求項１～６のうちの１つに記載の方法。
【請求項８】
　上記要求側エンティティの上記予め割り当てられた証明書及び上記提供側エンティティの上記予め割り当てられた証明書は、上記乗物の外部の認証手段によって発行され、上記乗物の集中化された証明書レジスタに格納されるか、又は、各オンボード装置に複製され

る、
請求項７記載の方法。
【請求項９】
上記要求側エンティティ及び上記提供側エンティティの予め割り当てられた証明書の存在及び相互の有効性を検証することは、それに関連付けられたディジタル署名の正確性を、マスター証明書に含まれる公開鍵を用いて検証することで行なわれ、上記マスター証明書の完全性及び真正性は外部機構によって保証される、
請求項７又は８記載の方法。
【請求項１０】
上記認証応答メッセージは、上記提供側エンティティの秘密暗号鍵を用いて生成された上記提供側エンティティの制御署名をさらに含む、
請求項７記載の方法。
【請求項１１】
サービスの同じインスタンスを要求する複数のエンティティは、上記サービスのインスタンスをマルチキャスト通信構成で提供する単一のエンティティと通信し、上記マルチキャスト通信構成では、上記サービスインスタンスに関連付けられた上記対称暗号鍵は、上記提供側エンティティによって生成され、上記複数の要求側エンティティによって共用される、
請求項３記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して、乗物のオンボードネットワークにおけるデータ又はメッセージの伝送に関し、より詳しくは、ＳＯＭＥ／ＩＰ通信プロトコルを用いた乗物のオンボードネットワークにおけるデータ又はメッセージの伝送に関する。
【０００２】
具体的には、本発明は、請求項１のプリアンブルに係る方法であって、乗物のオンボードネットワークにおいて、ＳＯＭＥ／ＩＰ通信プロトコルを用いて、サービスインスタンスを要求する少なくとも１つのエンティティと、サービスインスタンスを提供するエンティティとの間でデータ又はメッセージを伝送する方法に関する。
【背景技術】
【０００３】
ＳＯＭＥ／ＩＰ（Scalable service-Oriented MiddlewarE over IP：ＩＰ上のスケーラブルなサービス指向ミドルウェア）は、乗物のオンボードで動作するイーサネットネットワークを介して、例えば、カメラからテレマティックのエンターテインメント及び情報装置までに至る、異なるサイズ、機能、及びオペレーティングシステムを有する装置の間でメッセージ及び通信情報を伝送するために自動車セクタ用に開発された通信プロトコルである。ＳＯＭＥ／ＩＰプロトコルは、サービス指向の通信を提供し、各アプリケーションによってアプリオリに宣言されたサービスのリストに基づく。各アプリケーションについて、いわゆる「マニフェスト」が存在し、ここでは、提供されるすべてのサービスと、アプリケーションがアクセスを必要とするサービスとが記述される。サービス、又はそれが提供するデータは、提供側装置がメッセージを周期的に、又は状態変化が生じたときに送信するイベントに続いて、又は、要求側装置によって行われた要求、又は提供側装置における遠隔手続き呼び出しの後に、乗物のオンボード通信ネットワークに接続された装置によってアクセスされてもよい。
【０００４】
ＳＯＭＥ／ＩＰプロトコルは、インターネットプロトコル（ＩＰ）に基づく通信ネットワークを介して配送される複数のプロトコルデータ単位（protocol data unit：ＰＤＵ）にデータをシリアル化し、ＵＤＰ又はＴＣＰメッセージのペイロードとすることに基づく。
【先行技術文献】

【非特許文献】
【０００５】
【文献】"Specification of manifest AUTOSAR AP Release 17-10", October 17, 2017
【文献】J. Kreissl, "Absicherung der SOME/IP Kommunikation bei Adaptive AUTOSAR", November 15, 2017
【発明の概要】
【発明が解決しようとする課題】
【０００６】
現在、ＳＯＭＥ／ＩＰプロトコルは、乗物の内部での情報の交換におけるセキュリティの欠如により特徴付けられ、このため、外部装置はオンボード伝送手段へのアクセスを得る可能性があり、また、そこから、メッセージを傍受する可能性があり、２つのエンティティ間で交換される情報にアクセスすること、あるいは、受信側エンティティに偽メッセージを送信し、偽造された伝送について受信側エンティティに気づかせることなく送信側エンティティの役割になりすますことの可能性がある。
【０００７】
非特許文献１及び２は、ＴＬＳプロトコルを用いてＳＯＭＥ／ＩＰメッセージをカプセル化することを提案している。しかしながら、ＴＬＳプロトコルは、ユニキャスト伝送を保護することのみを意図し、伝送プロトコルに特異的である。
【０００８】
通信において、認証（authentication）は、主体／エンティティの身元（識別情報）を検証する処理を示す。それに代わって、認可（authorization）は、主体／エンティティが何の実行を許可されているかを決定するルールを示す。これら２つの概念は互いに直交かつ独立であるが、両者は、安全に動作するシステムの設計において重要である。従来技術において、ユーザ認証は、通常、予め決められた動作を実行することを特定のエンティティに認可するための要件である。
【０００９】
ＴＬＳプロトコルにおいて、互いに通信する複数のエンティティの認証は、ディジタル証明書を用いて実装される。セッションを確立する初期ステップの間、サーバ及びクライアントは、それらのディジタル証明書を、証明書の正当な所持者であることの証明とともに、互いに提示するように要求される。この目的のために、ディジタル証明書は、検証されうる何らかの暗号学的パラメータ、例えば公開鍵を識別情報に関連付けるために使用される。しかしながら、ＴＬＳプロトコルは、ディジタル証明書の内容にいかなる意味付けを行う手段も持たない。従って、互いに通信しているエンティティが認証されることを可能にするが、ＴＬＳプロトコル自体は、エンティティが通信の開始も認可されているか否かを検証することができない。実際、この検証は、より高レベルのプロトコル及びアプリケーションに残される。
【００１０】
前述の文献は、ＴＬＳプロトコルを用いて異なる装置間に安全（セキュア）な通信経路を確立することを提案し、サーバ及びクライアント側の証明書を用いて相互認証を達成することを示唆する。ディジタル証明書の有効性を検証すること以外に、さらなる検証は実行されない。
これらの文献は、２つのエンティティ間の通信が許可されるべきであるか否かを検証する方法、すなわち、アプリケーションが認可されていないサービスにアクセスすることを防ぐ方法についてさらなる詳細事項を提供しない。
【００１１】
ＴＬＳプロトコル自体は、いくつかの欠点を有する。複数レベルのセキュリティは、最新バージョンの標準（ＴＬＳ１．３）によって公式にはサポートされず、したがって、それは実際、より高コストな「機密（confidentiality）」セキュリティレベルに限定される。認証のみのモードにおいて動作する一組の暗号スイートをサポートするＴＬＳ１．２標準のバージョンを適用することを仮定しても、セキュリティレベルは、設計者及び開発

者が望むであろうセキュリティのレベルを実際に守るという保証がない、何らかの変更可能なローカルパラメータ（許可された一組の暗号化スイート）に依存するであろう。

【００１２】

しかしながら、従来のインターネットサーバとは異なり、自動車のＥＣＵは、乗物において物理的にアクセス可能であり、保護されていない設定ファイルの内容を編集することが容易になる。

【００１３】

本発明の目的は、乗物通信ネットワーク内において情報の安全な交換を可能にする、ＳＯＭＥ／ＩＰプロトコルの拡張を提供することである。

【課題を解決するための手段】

【００１４】

本発明によれば、この目的は、請求項１に記載された特徴を有する、乗物のオンボード通信ネットワークにおいてデータ又はメッセージを伝送する方法によって達成される。

【００１５】

特定の実施形態は従属請求項の主題であり、その内容は、本明細書の主要部分として理解されるべきである。

【００１６】

要約すると、本発明は、所与のサービスのインスタンスを要求するどのエンティティが、また、所与のサービスのインスタンスを提供するどのエンティティが、乗物のオンボードで互いに通信する（トラフィック行列）ように認可されているのかを証明する原理に基づき、それによって、各サービスは、又は、実行されることでサービスを行う各アプリケーションは、認可されたエンティティによってのみアクセスされうる。エンティティは、オンボード装置であるか、又は、オンボード装置によって実行されるアプリケーションである。サービスを要求又は提供する乗物のオンボードのエンティティ、すなわち、オンボード装置、又は、複数の実行可能な機能のうちで予め決められた機能を実行する装置によって使用される特定のアプリケーションの認可は、乗物の外部の認証手段によって、例えば、乗物の製造業者又はオンボード構成要素の一次サプライヤによって証明される。

【００１７】

サービスインスタンスを要求又は提供する乗物のエンティティを認可することは、サービスインスタンスを要求するエンティティ及びサービスインスタンスを提供するエンティティの両方によって相互に検証され、両方のエンティティの認可の検証が肯定的な結果をもたらしている場合、認証コードは、関与するエンティティ間における後続の任意の通信メッセージであって、ＳＯＭＥ／ＩＰプロトコルに従って定義され、提供側エンティティ及び要求側エンティティの間で伝送されるメッセージに関連付けられる。

【００１８】

認証コードは、保護されるメッセージとサービスインスタンスに関連付けられた対称暗号鍵とを入力として受けて固定サイズのバイト列を出力として返す暗号化関数を用いて、送信側エンティティによって生成される。関連するサービスインスタンスに関連付けられた対称鍵であって、通信を開始する前、通信セッションを確立するステップの間に、認可されたエンティティ間で交換される対称鍵が使用される。これにより、受信側エンティティは、同じ対称鍵を所有することで、メッセージがその生成以来変更されていないこと（完全性）と、対称鍵を認識しているエンティティによって生成されたこと（認証）とを検証することができる。

【００１９】

従って、本発明の解決方法は、その優位点として、通信しているエンティティの認証機能と、各安全な通信セッションの確立中に通信を開始する認可との両方を達成するために、ＳＯＭＥ／ＩＰミドルウェアでの統合を使用する。従来技術とは異なり、各異なるＳＯＭＥ／ＩＰサービスインスタンスのために異なる安全なセッションが確立されなければならず、すなわち、本発明の解決方法は、サービスインスタンスの粒度で動作する。

【００２０】

各アプリケーション（又はオンボード装置）は、認証の目的で、異なるディジタル証明書に関連付けられる。さらに、同じディジタル証明書は、アプリケーション（又はオンボード装置）が提供／要求することが認可されている一組のサービスを宣言するように拡張される。このように、自動車製造業者が、許可されるトラフィック行列を定義し、実際に確立されうる通信の集合全体を宣言するために、ディジタル証明書が使用されうる。

【００２１】

サービスにアクセスすることを希望するアプリケーションによって新たな通信が開始されるときはいつでも、ＴＬＳプロトコルと同様に証明書の交換が行われる。ＴＬＳプロトコルと同様に、通信を要求するエンティティによって提示されたディジタル証明書の有効性が最初に検証される。ＴＬＳプロトコルとは異なり、本発明はまた、現在のサービスインスタンスと、その証明書において宣言されたルールとの対応を検証し、エンティティが通信を開始することも認可されているか否かを検証するように構成される。言いかえると、アプリケーションデータを交換する前、安全なセッションの確立中に、サービスインスタンスにアクセスする認証及び認可の両方が本発明の方法に従って検証される。

【００２２】

優位点として、本発明によれば、必要性に応じて、乗物の異なるオンボードエンティティ間の通信に少なくとも２レベルのセキュリティをそれぞれ提供することができる。第１のセキュリティレベル「認証」では、受信側エンティティに到達したメッセージが、証明された（認可された）エンティティから発信され、かつ、ネットワークを介する伝送中に変更されなかったことが保証される。第２の、より高いセキュリティレベル「機密」では、認可されていないサードパーティーがネットワークを介して伝送中のメッセージの内容を復号することは防止される。

【００２３】

具体的には、「認証」セキュリティレベルは、認可されたエンティティのみが、特定のサービスに関連付けられたメッセージを送信しうることを保証し、メッセージ認証を提供する。提供側エンティティ及び要求側エンティティのいずれであれ、送信側エンティティによって、サービスインスタンスに関連するメッセージを含むＳＯＭＥ／ＩＰプロトコルに係るパケットが送信される前に、それに対して、対称暗号化機構を用いて生成された認証コード（ＭＡＣ）が付加される。受信側エンティティがメッセージを受信するとき、このコードが検証されてもよく、検証に成功した場合、受信側エンティティは、メッセージが、信頼できる証明された（認可された）送信側エンティティから発信され、ネットワークを介する伝送中に変更されていないと決定してもよい。言いかえると、受信側エンティティは、メッセージの真正性及び完全性を信頼しうる。さらに、前述の認証コードによってその信頼性が保証される連続番号をサポートデータフィールドに追加することによって、複製による攻撃を防ぐことができる。複製による攻撃は、有効な情報パケットを傍受し、その後、サードパーティーにより、同じ動作を新たに要求する同じパケットを再送信することで特徴付けられる。「認証」セキュリティレベルの場合には、第３のエンティティは、乗物通信ネットワークにおいて伝送される情報を傍受できるが、偽メッセージを挿入することはできない。偽メッセージは、提供側及び要求側エンティティの相互の認識の後に交換された暗号鍵を用いて生成されるメッセージ認証コードをもたないので、容易に検出可能であり、従って、受信側エンティティによって無視されうる。このモードは、サードパーティーが偽コマンドにより乗物のオンボードで危険かもしれない物理的動作をトリガすることを防ぐ重要性と、計算及び伝送リソースを保護するために、交換されたデータが機密ではない可能性とのバランスをとる。

【００２４】

「機密」セキュリティレベルは、上述の「認証」セキュリティレベルによって提供されるすべての特性を含む、すなわち、それは、乗物通信ネットワークにおいて交換されるメッセージの真正性及び完全性を保証し、複製による攻撃を防ぐ。さらに、各メッセージの伝送が行われる前に、メッセージのペイロードは暗号化関数で暗号化され、認可されていないエンティティがそれにアクセスすることを防ぐ。このことは、機密性、すなわちデー

タの秘密を保証する。従って、乗物通信ネットワークへの侵入を試みるサードパーティーは、認証コードの検証によってメッセージが認識されるので、ネットワークにメッセージを挿入することができず、また、メッセージのセマンティックな意味を解読するための必要な鍵をもたず、伝送されたデータを復号することもできない。このモードは、特にメッセージ伝送の待ち時間に関して、より高い計算上の負荷がかかるものの、最高レベルのセキュリティを提供する。

【００２５】

サポートデータフィールドは、優位点として、連続番号に加えて、選択された対称暗号アルゴリズムによって必要とされる他の任意のパラメータ、例えば初期化ベクトルを含んでもよい。初期化ベクトルは連続番号と一致してもよい。

【図面の簡単な説明】

【００２６】

【図１】乗物通信ネットワークにおける、サービスを要求するエンティティ又はクライアントと、サービスを提供するエンティティ又はサーバとの間の既知の通信モードを示す図である。

【図２】ＳＯＭＥ／ＩＰプロトコルに従って乗物通信ネットワークを介して伝送される、ヘッダ及びペイロードを含むメッセージの既知のフォーマットを概略的に示す図である。

【図３】本発明が関連する、乗物通信ネットワークを介するマルチキャスト通信構成を概略的に表す図である。

【図４】本発明に係る、乗物の通信ネットワークに接続された要求側エンティティ及び提供側エンティティの間における通信セッションの確立の上位概念を表す図である。

【図５】本発明に係る乗物通信ネットワークに接続された乗物エンティティの特性、又は乗物エンティティによって実行されるアプリケーションの特性の宣言を概略的に表す図である。

【図６】本発明の方法に係る、サービスインスタンスを要求するエンティティと、サービスインスタンスを提供するエンティティとの間における相互認証シナリオを表すシーケンス図である。

【図７】本発明の方法に係る認証要求メッセージのフォーマットの例を概略的に示す図である。

【図８】本発明の方法に係る認証応答メッセージのフォーマットの例を概略的に示す図である。

【図９】本発明に係る改善されたＳＯＭＥ／ＩＰプロトコルに従って乗物ネットワークを介して伝送されるメッセージのフォーマットの例を概略的に示す。

【発明を実施するための形態】

【００２７】

本発明の別の特徴及び利点は、以下のある実施形態の詳細な説明から、添付された図面を参照して、非限定的な例示によって与えられて、より明らかになるであろう。

【００２８】

図１は、サーバエンティティ又は提供側エンティティＯＦと、クライアントエンティティ又は要求側エンティティＲＱとの間における、２つの異なるタイプの通信を示す。「要求／応答」と呼ばれる第１のタイプの通信は、要求側エンティティＲＱによってサービスインスタンスに対する要求を送信することを含み、オプションで、その結果として、提供側エンティティＯＦによって応答を送信することを含む。「発行／加入」と呼ばれる第２のタイプの通信は、要求側エンティティＲＱによって、サービスインスタンスに関連付けられた１つ又は複数のイベントへの加入を起動することと、提供側エンティティＯＦによって、周期的な通知又はイベントによりトリガされた通知を送信することとを含む。

【００２９】

図２は、ＳＯＭＥ／ＩＰプロトコルに従って乗物通信ネットワークを介して伝送されるメッセージのフォーマットを示す。メッセージは、メッセージ識別子と、メッセージ長と、要求識別子と、プロトコルバージョン、インターフェースバージョン、メッセージタイ

プ、及びリターンコードの複数の識別情報フィールドとを含むヘッダＨを含む。メッセージは、可変サイズのペイロードＰも含む。

【００３０】

図３は、乗物通信ネットワークにおけるマルチキャスト通信構成を概略的に表し、同じサービスインスタンスを要求する複数のエンティティＲＱは、サービスインスタンスを提供する単一のエンティティＯＦと通信する。連続線の矢印ＡｕｔｈＲＥＱ及びＡｕｔｈＲＥＳは、相互認証の双方向通信を表し、一方、破線の矢印Ｍは、相互認証に成功した場合にのみ可能になる、本発明の安全なＳＯＭＥ／ＩＰプロトコルによるメッセージ通信セッションを表す。

【００３１】

図４は、非対称暗号化技術を用いた相互認証によって特徴付けられる、乗物の通信ネットワークに向かう要求側エンティティＲＱ及び提供側エンティティＯＦの間における通信セッションの確立を概略的に表す。要求側エンティティＲＱは、提供側エンティティＯＦのサービスインスタンスを要求するとき、ＡＵＴＨ＿ＲＱ認証及び認可証明書を送信し、後者は、暗号化された形式の対称暗号鍵Ｋとともに、ＡＵＴＨ＿ＯＦ認証及び認可証明書を送信することで応答する。

【００３２】

図５は、乗物通信ネットワークに接続された乗物エンティティＥの特性、又は乗物エンティティＥによって実行されるアプリケーションの特性の宣言を概略的に表す。エンティティＥ、又はエンティティＥによって実行されるアプリケーションは、各最低セキュリティレベルＳＬ１，ＳＬ２，ＳＬ３をそれぞれ有する複数のサービスＳ１，Ｓ２，Ｓ３を提供してもよく、また、各最低セキュリティレベルＳＬ４，ＳＬ５をそれぞれ有する複数のサービスＳ４，Ｓ５を要求してもよい。そのようなエンティティ又はアプリケーションは、証明書フィンガープリントＦ及び署名Ｓに関連付けられる。証明書フィンガープリントは、例えばＸ．５０９標準に係る証明書Ｃであってもよく、又は、例えば、乗物の製造業者又はオンボード構成要素の一次サプライヤのような、乗物の外部の証明手段によって発行され、乗物の集中化された証明書レジスタＲＥＧを指し示すように適応化されるか、又は、各オンボード装置に複製された（後者の場合、証明書が要求されたときにローカルに利用可能であるので、より高い効率をもたらす）証明書識別子Ｆ＿ＩＤ＃（ここで、＃＝１，２，…）であってもよい。各証明書Ｃ＃（ここで、＃＝１，２，…）は、既知の非対称暗号化技術に従って要求側及び提供側エンティティＲＱ，ＯＦの間で交換されるデータの暗号化及び復号のために、対応する秘密暗号鍵Ｋ＿ＰＲＩＶとともに機能するように適応化され、対応するエンティティによってのみアクセス可能である公開暗号鍵Ｋ＿ＰＵＢを含む。証明（すなわち、証明書の存在及び有効性）は、サービスインスタンスを要求するエンティティと、サービスインスタンスを提供するエンティティとの認可を、乗物のオンボードで互いに通信するために証明する。サービス、又は実行することでサービスを生成するアプリケーションは、認可されたエンティティによってのみアクセスされてもよい。

【００３３】

図６～図９を参照して、本発明に係るＳＯＭＥ／ＩＰプロトコルによる安全な通信方法について、以下に説明する。

【００３４】

図６は、要求側エンティティＲＱ及び提供側エンティティＯＦの間における相互認証シナリオのシーケンス図を示す。最初のステップにおいて、要求側エンティティＲＱは、乗物通信ネットワークにおいて、サービスインスタンスを要求しようとしている相手の提供側エンティティＯＦに、ＡｕｔｈＲＥＱ認証要求メッセージを送信する。図７に、ＡｕｔｈＲＥＱ認証要求メッセージの可能なフォーマットを示す。それは、特に、要求側エンティティＲＱのＦ＿ＲＱ証明書フィンガープリントを含む。

【００３５】

ＡｕｔｈＲＥＱ認証要求メッセージを受信したとき、提供側エンティティＯＦは、例えば、ＲＥＧ証明書レジスタを介して証明書にアクセスし、証明書識別子Ｆ＿ＲＱに関連付

けられたアドレスにおいて調べることで、Ｆ＿ＲＱフィンガープリントを介して要求側エンティティの証明書を検索する。提供側エンティティは、外部機構を介して保証される完全性及び真正性を有する、「ルート証明書」と呼ばれるマスター証明書に含まれる公開鍵を用いて、証明書に含まれるディジタル署名を検証することで証明書を検証し、成功した場合、証明書によって表される要求側エンティティによって許可される最低セキュリティレベルSL_{RQ}を、サービスインスタンスが現在提供されるセキュリティレベルSL_{SE}に対して比較する。要求側エンティティによって許可される最低セキュリティレベルSL_{RQ}が、サービスインスタンスが提供されるセキュリティレベルよりも高い場合、すなわち、$SL_{RQ}>SL_{SE}$の場合、提供側エンティティＯＦは通信を異常終了させる。そうでなければ、要求側エンティティによって許可される最低セキュリティレベルSL_{RQ}が、サービスインスタンスが提供されるセキュリティレベルSL_{SE}以下である場合、提供側エンティティＯＦは、乗物通信ネットワークにおいてＡｕｔｈＲＥＳ認証応答メッセージを送信することで応答する。

【００３６】

図８に、ＡｕｔｈＲＥＳ認証応答メッセージの可能なフォーマットを示す。それは、特に、提供側エンティティＯＦの証明書フィンガープリントＦ＿ＯＦと、ｋ＝ｅｎｃｒｙｐｔ（Ｋ＿ＳＹＭ）$_{K_PUB_RQ}$で表される、要求側エンティティの証明書から取得された要求側エンティティＲＱの公開暗号鍵Ｋ＿ＰＵＢ＿ＲＱによって暗号化された対称暗号鍵Ｋ＿ＳＹＭと、ｓ＝ｓｉｇｎ（ＡｕｔｈＲＥＳ）$_{K_PRIV_OF}$で表される、提供側エンティティＯＦの秘密暗号鍵によって付加されたディジタル署名Ｓ＿ＯＦとを含む。

【００３７】

ＡｕｔｈＲＥＳ認証応答メッセージを受信したとき、要求側エンティティＲＱは、例えば、ＲＥＧ証明書レジスタを介して証明書にアクセスし、証明書識別子Ｆ＿ＯＦに関連付けられたアドレスにおいて調べることで、Ｆ＿ＯＦフィンガープリントを介して提供側エンティティの証明書を検索する。要求側エンティティは、外部機構を介して保証される完全性及び真正性を有する、「ルート証明書」と呼ばれるマスター証明書に含まれる公開鍵を用いて、証明書に含まれるディジタル署名を検証することで証明書を検証し、成功した場合、提供側エンティティの証明書から取得された提供側エンティティＯＦの公開暗号鍵Ｋ＿ＰＵＢ＿ＯＦによって、受信されたメッセージに関連付けられた署名ｓを検証する。ディジタル署名の検証に成功した場合、要求側エンティティは、サービスインスタンスが現在提供されるセキュリティレベルSL_{SE}を、証明書によって表された提供側エンティティによって保証されなければならない最低セキュリティレベルSL_{OF}と、それ自体の許可された最低セキュリティレベルSL_{RQ}との両方に対して比較する。サービスインスタンスが提供されるセキュリティレベルが、提供側エンティティによって保証されなければならない最低セキュリティレベルSL_{OF}より低い場合、すなわち、$SL_{SE}<SL_{OF}$の場合、又は、サービスが提供されるセキュリティレベルが、その許可された最低セキュリティレベルSL_{RQ}より低い場合、すなわち、$SL_{SE}<SL_{RQ}$の場合、要求側エンティティは通信を異常終了させる。逆の場合、すなわち、サービスインスタンスが提供されるセキュリティレベルが、提供側エンティティによって保証されなければならない最低セキュリティレベルSL_{OF}と、それ自体の許可された最低セキュリティレベルSL_{RQ}との両方以上である場合、要求側エンティティＲＱは、式Ｋ＿ＳＹＭ＝ｄｅｃｒｙｐｔ（ｋ）$_{K_PRIV_RQ}$で簡潔に示されるように、後のメッセージの保護のために提供側エンティティによって送信された対称鍵を、要求側エンティティＲＱの秘密暗号鍵を用いて復号することで、通信セッションの確立を完了する。

【００３８】

サービスインスタンスを要求又は提供する乗物のエンティティを認可することは、次いで、関連する証明書を検証することにより、サービスインスタンスを要求するエンティティ及びサービスインスタンスを提供するエンティティの両方によって相互に検証され、両方のエンティティの認可の検証が肯定的な結果をもたらしている場合、認証コードは、関与するエンティティ間における後続の任意の通信メッセージであって、ＳＯＭＥ／ＩＰプ

ロトコルに従い、提供側エンティティ及び要求側エンティティの間で伝送されるメッセージに関連付けられる。

【００３９】

いったん要求側エンティティＲＱ及び提供側エンティティＯＦの間における通信セッションが確立されると、メッセージは、図９に示すフォーマットに従って、２つの認証及び認可されたエンティティ間において、ＳＯＭＥ／ＩＰ通信プロトコルに従って安全に交換されうる。ここで、「機密」の通信が進行中である場合、ペイロードＰは対称鍵Ｋ＿ＳＹＭを用いて暗号化されている

【００４０】

優位点として、説明した方法は、マルチキャスト通信構成において、各サービスインスタンスのために異なる対称鍵を用いたメッセージの保護を保証する。鍵は、通信セッションを確立するステップの間に、提供側エンティティによって生成され、多数の要求側エンティティと安全に共用される。鍵の再生成は、永続的なサービス、例えば位置データの通信のために便利である可能性があり、また、例えば、使用される暗号アルゴリズム及び鍵の特徴によって保証されるセキュリティのレベルを所定時間にわたって保つために、周期性に実行されるべきである。

【００４１】

予め決められたサービスインスタンスに関係する通信を行う特定のエンティティのグループにおいて単一の鍵を使用することで、ＳＯＭＥ／ＩＰプロトコルの機能を制限することなく、また、乗物通信ネットワークの使用を増大させることなく、マルチキャスト通信を透過的に保護することができる。

【００４２】

優位点として、本発明の方法は、好ましくはサービスインスタンスのレベルの粒度で動作するように、すなわち、ＳＯＭＥ／ＩＰサービスの各インスタンスを、予め決められたアプリケーション（又はオンボード装置）がアクセスしうる、又はアクセス拒否されうる一意のオブジェクトとみなして動作するように設計される。この状態は、極めて微細な粒度の採用を必要とする、通信の強い隔離の必要性と、乗物通信ネットワークを介するメッセージ及びデータの伝送の待ち時間における持続不可能な増大を引き起こさないように、認証セッションを確立するプロセス数の制限を必要とする、リソースへの配慮との間における効率的な妥協点である。

【００４３】

ＴＬＳプロトコルとは異なり、本発明の方法は、ディジタル証明書が、各オンボードアプリケーション又は装置がアクセスするように認可された一組のサービスインスタンスを定義すること（トラフィック行列）に加えて、各エンティティによって守られなければならない最低レベルのセキュリティを宣言するように構成することで、アプリケーション又はオンボード装置の設計者によって構成されるセキュリティのレベルを厳格に守るように設計される。従って、通信セッションを確立するステップの間、所望のサービスインスタンスが提供されるレベルは、提供側エンティティ及び要求側エンティティの要件と比較され、これにより、これらのエンティティが、以前に課された設計上の制約を破ることを防ぐ。ディジタル証明書の真正性及び完全性が保証されていると仮定すると、本発明の方法は、アプリケーション又はオンボード装置の設計者によって課された要件よりもセキュリティレベルを強制的な劣化させることに基づく攻撃を防ぐ。

【００４４】

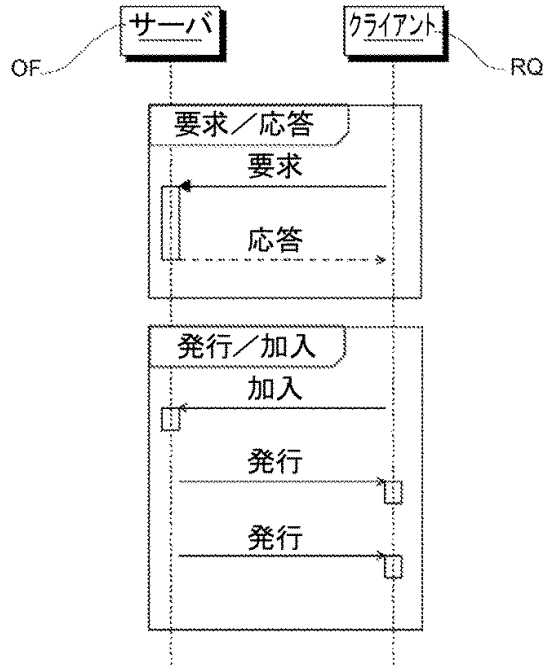
従って、本発明は、外部ソリューションによって課される制約を緩和するように、また、ＳＯＭＥ／ＩＰプロトコルによってサポートされる異なるすべての通信モデル（ユニキャスト及びマルチキャスト）との適合性を達成するように、ＳＯＭＥ／ＩＰプロトコルへ一体化された個人化されたアプローチを表す。それは、ある乗物において許可されるトラフィック行列（各エンティティが要求／提供しうる一組のサービス）を表し、それと同時に、発生しうる異なるセキュリティ及びオーバーヘッド要求を考慮して複数レベルのセキュリティを提供するための、簡単かつ有効な解決方法を提供する目的を達成する。

【００４５】

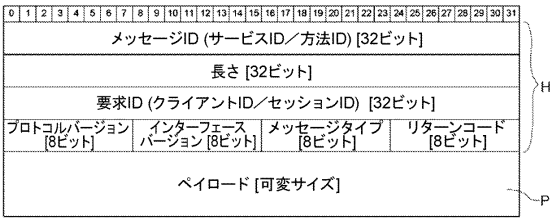
当然ながら、理解される本発明の原理、製造上の詳細事項、及び実施形態は、添付された特許請求の範囲に定義される本発明の範囲から外れることなく、非限定的な例としてのみ説明及び図示したものに比較して大きく変化してもよい。

【図面】

【図１】



【図２】



【図３】

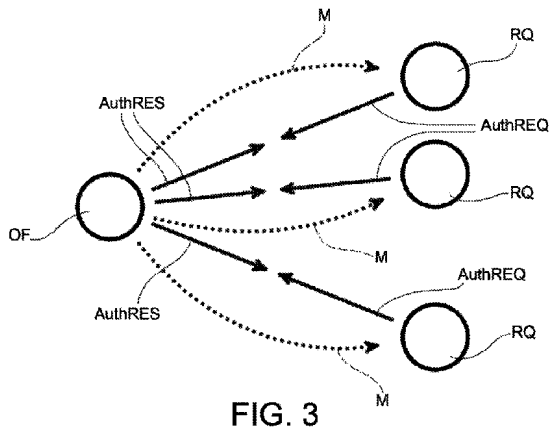


FIG. 3

【図４】

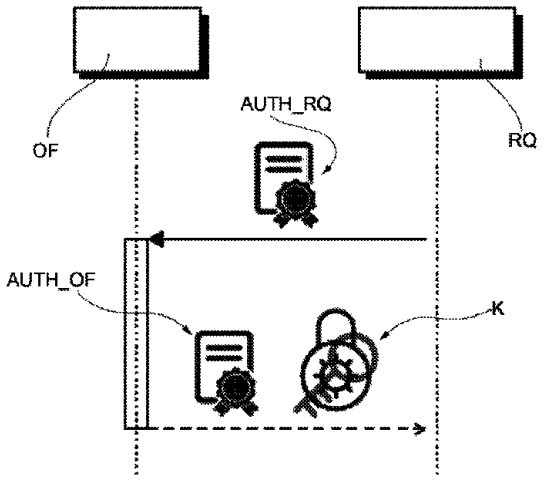
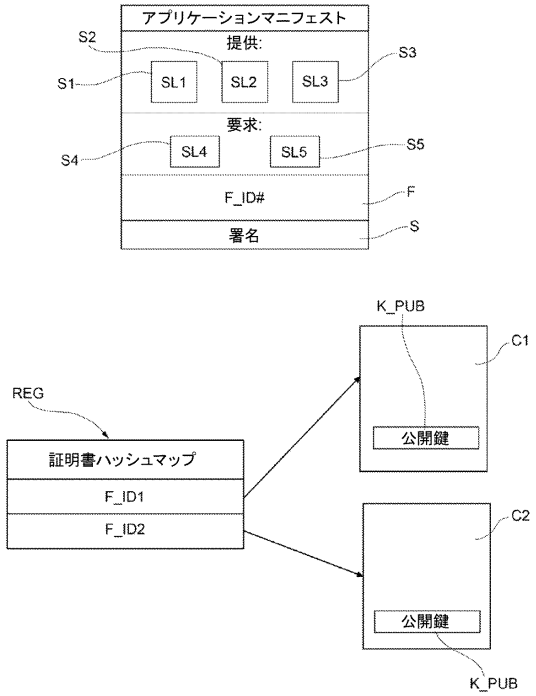
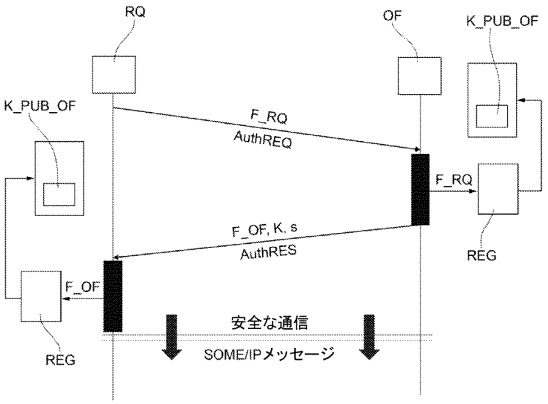


FIG. 4

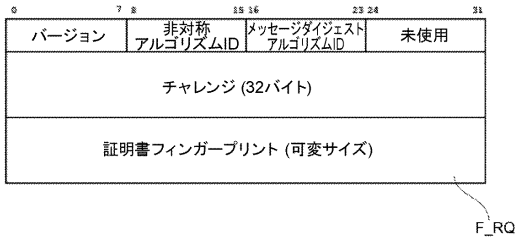
【図５】


アプリケーションマニフェスト
提供:
SL1
SL2
SL3
要求:
SL4
SL5
F_ID#
署名
S1
S2
S3
S4
S5
F
S
REG
証明書ハッシュマップ
F_ID1
F_ID2
K_PUB
公開鍵
C1
C2
K_PUB

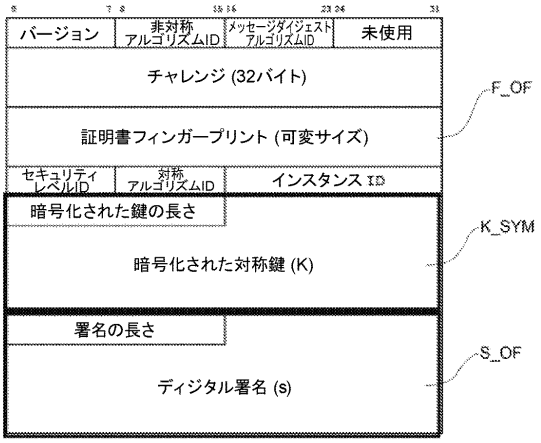
【図６】


RQ
OF
K_PUB_OF
K_PUB_OF
F_RQ
AuthREQ
F_RQ
REG
F_OF, K. s
AuthRES
F_OF
REG
安全な通信
SOME/IPメッセージ

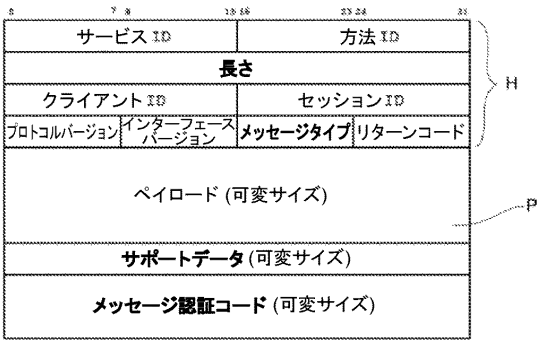
【図７】


0
7
8
15
16
23
24
31
バージョン
非対称
アルゴリズムID
メッセージダイジェスト
アルゴリズムID
未使用
チャレンジ (32バイト)
証明書フィンガープリント (可変サイズ)
F_RQ

【図８】


0
7
8
15
16
23
24
31
バージョン
非対称
アルゴリズムID
メッセージダイジェスト
アルゴリズムID
未使用
チャレンジ (32バイト)
証明書フィンガープリント (可変サイズ)
F_OF
セキュリティ
レベルID
対称
アルゴリズムID
インスタンス ID
暗号化された鍵の長さ
暗号化された対称鍵 (K)
K_SYM
署名の長さ
ディジタル署名 (s)
S_OF

【図９】


サービス ID
方法 ID
長さ
クライアント ID
セッション ID
プロトコルバージョン
インターフェースバージョン
メッセージタイプ
リターンコード
H
ペイロード (可変サイズ)
P
サポートデータ (可変サイズ)
メッセージ認証コード (可変サイズ)

フロントページの続き

(72)発明者　リッソ，フルヴィオ
イタリア、イ－１２０３０マンタ（クーネオ）、ヴィア・マッテオッティ６３
(72)発明者　ヴァレンツァ，フルヴィオ
イタリア、イ－１０１４１トリノ、ヴィア・マルタ３６
(72)発明者　シスト，リッカルド
イタリア、イ－１０１２９トリノ、コルソ・ドゥーカ・デッリ・アブルッツィ２４、ポリテクニコ・ディ・トリノ内
(72)発明者　イオーリオ，マルコ
イタリア、イ－１００６８ヴィッラフランカ・ピエモンテ（トリノ）、ヴィア・クワトロ・ノヴェンブレ２３
(72)発明者　レイネリ，マッシモ
イタリア、イ－１０１４３トリノ、ヴィア・ロソリーノ・ピロ４４
(72)発明者　ブッティリエーリ，アルベルト
イタリア、イ－１００７９マッパーノ（トリノ）、ヴィア・ブオナッローティ２１／ア

審査官　行田 悦資
(56)参考文献　特開２０１７－０７９３６９（ＪＰ，Ａ）
特開２０１５－００７９７８（ＪＰ，Ａ）
特開２００４－２６６３４２（ＪＰ，Ａ）
米国特許出願公開第２０１２／０２４０２１２（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３６
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　９／０８